#4

S&H Form: (2/01)

Attorney Docket No. 1083.1081

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Kiyotaka KINOSHITA

Application No.: Group Art Unit:

Filed: June 8, 2001 Examiner:

For: CRISIS MANAGEMENT SYSTEM, COMPUTER, AND COMPUTER MEMORY PRODUCT

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-177635

Filed: June 13, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 6/8/01

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

PATENT OFFICE

JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: June 13, 2000

Application Number: Patent Application No. 2000-177635

Applicant (s): FUJITSU LIMITED

April 27, 2001

Commissioner, Patent Office

Kozo OIKAWA

[Name of Document] Patent Application
[Reference Number] 0090108
[Date of Filing] June 13, 2000
[Destination] Commissioner, Patent Office
[International Patent Classification] G06F 7/00
G06F 12/00 511
G06F 12/00 514
[Title of Invention] CRISIS MANAGEMENT SYSTEM AND COMPUTER
[Number of Claimed Inventions] 5
[Inventor]
[Address] c/o FUJITSU LIMITED,
1-1, Kamikodanaka 4-chome, Nakahara-ku,
Kawasaki-shi, Kanagawa
[Name] Kiyotaka KINOSHITA
[Applicant]
[Identification Number] 000005223
[Name] FUJITSU LIMITED
[Attorney]
[Identification Number] 100078868
[Patent Attorney]
[Name] Takao KOHNO
[Telephone Number] 06-6944-4141
[Indication of Official Fee]
[Register Number] 001889
[Amount] ¥21,000
[List of Annexes]
[Name of Article] Specification 1
[Name of Article] Drawings 1
[Name of Article] Abstract 1
[Number of General Authorization] 9705356
[Proof] Needed

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年 ６月１３日

出願番号
Application Number: 特願２０００－１７７６３５

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ４月２７日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号 出証特２００１－３０３６９６３

【書類名】　特許願

【整理番号】　0090108

【提出日】　平成12年 6月13日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 7/00

G06F 12/00 511

G06F 12/00 514

【発明の名称】　危機管理システム及びコンピュータ

【請求項の数】　5

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　木下　清孝

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100078868

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　06-6944-4141

【手数料の表示】

【予納台帳番号】　001889

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705356

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　危機管理システム及びコンピュータ

【特許請求の範囲】

【請求項１】　通信網を介して接続されるサーバコンピュータと端末装置との間で実行され、所定の事象の発生により所要の情報を送受信する危機管理システムにおいて、

前記サーバコンピュータは、

事象に関する情報を受け付ける情報受付手段と、

事象の種類と該事象毎の特性情報を登録した特性登録ファイルと、

事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録した対処情報ファイルと、

前記情報受付手段により受け付けた情報と前記特性登録ファイルとを比較して、事象を特定する特定手段と、

該特定手段により特定した事象についての、前記対処情報ファイルに登録した提供情報項目に係る提供情報を収集する情報収集手段と

を備え、

前記端末装置は、

管理者に付与される固有の識別子を受け付ける識別子受付手段と、

管理者の人体特徴情報を受け付ける人体特徴情報受付手段と、

前記識別子受付手段で受け付けた識別子及び前記人体特徴情報受付手段により受け付けた人体特徴情報を前記サーバコンピュータへ送信する識別情報送信手段と

を備え、

前記サーバコンピュータは、更に、

管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録してある認証データファイルと、

前記識別情報送信手段により送信された管理者の識別子及び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行う認証手段と、

前記特定手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証手段により認証した管理者のアクセス許可レベルに基づいて提供情報に対するアクセスを許可するか否かを判断する判断手段と、

該判断手段によりアクセスを許可すると判断した場合は、前記情報収集手段で収集した前記提供情報項目に係る提供情報を前記端末装置へ送信する提供情報送信手段と

を備えることを特徴とする危機管理システム。

【請求項２】　前記対処情報は前記複数の提供情報項目を提供すべき順序情報を更に含み、

前記提供情報送信手段は、

前記順序情報に従って前記提供情報を送信するよう構成してある

ことを特徴とする請求項１に記載の危機管理システム。

【請求項３】　前記識別情報送信手段は、

更に、前記端末装置のハードウェア情報を送信するよう構成してあり、

前記提供情報送信手段は、

前記判断手段によりアクセスを許可すると判断した場合は、前記提供情報送信手段により送信されたハードウェア情報に基づいて前記情報収集手段により収集した前記提供情報を編集した後に、前記端末装置へ前記編集後の提供情報を送信するよう構成してある

ことを特徴とする請求項１または２に記載の危機管理システム。

【請求項４】　他のコンピュータとの間で所定の事象の発生により所要の情報を送受信するコンピュータにおいて、

事象に関する情報を受け付ける情報受付手段と、

事象の種類と該事象毎の特性情報を登録した特性登録ファイルと、

事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録した対処情報ファイルと、

前記情報受付手段により受け付けた情報と前記特性登録ファイルとを比較して、事象を特定する特定手段と、

該特定手段により特定した事象についての、前記対処情報ファイルに登録した

提供情報項目に係る提供情報を収集する情報収集手段と、

管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録してある認証データファイルと、

前記他のコンピュータから送信された管理者の識別子及び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行う認証手段と、

前記特定手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証手段により認証した管理者のアクセス許可レベルに基づいて提供情報に対するアクセスを許可するか否かを判断する判断手段と、

該判断手段によりアクセスを許可すると判断した場合は、前記情報収集手段で収集した前記提供情報項目に係る提供情報を前記他のコンピュータへ送信する提供情報送信手段と

を備えることを特徴とするコンピュータ。

【請求項５】　他のコンピュータとの間で、事象の発生により必要な情報を送受信するコンピュータにおいて、

管理者に付与される固有の識別子を受け付ける識別子受付手段と、

管理者の人体特徴情報を受け付ける人体特徴情報受付手段と、

前記識別子受付手段で受け付けた識別子、前記人体特徴情報受付手段により受け付けた人体特徴情報及びハードウェア情報を送信する識別情報送信手段と

を備えることを特徴とするコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信網を介して接続されるサーバコンピュータと通信端末との間で実行され、所定の事象の発生により所要の情報を送受信する危機管理システム及びコンピュータに関し、特に空港で発生した事象をサーバコンピュータで管理し、空港外に設けられる通信端末へ緊急情報を提供する危機管理システム及びコンピュータに関する。

【０００２】

【従来の技術】

近年、危機管理の重要性が認識され、地震またはクーデタ等の事象（緊急事態）が発生した場合における、関係者への情報提供の迅速性が要求されている。例えば、空港等でハイジャックまたは事故が発生した場合は、被害状況、乗客の安否、乗客の名簿及び救急車または警察への手配等の情報を、収集すると共に空港外にいる管理者（例えば、運航管理者等）にその情報を迅速・的確に提供する必要がある。これは、国家レベルでの事象が発生した場合でも、共通していえることである。空港内の情報の管理は特開平９－１４７３００号公報に開示されているがこれはあくまで空港内の管理であり外部へ事象の情報を提供するものではなかった。

【０００３】

従来、事象の発生時は空港内にいるスタッフが被害状況等を収集整理し、空港外にいる管理者に電話等で被害状況等を口頭で伝えると共に、空港へ駆けつけるよう呼び出し、応対に当たることとしていた。

【０００４】

【発明が解決しようとする課題】

しかし、事象が発生し空港外にいる管理者へ必要な情報を提供する場合は、まず第１に迅速性が要求されるが、複数の管理者の全てに電話等で呼び出すのは時間がかかり、また確実性に欠けるという問題があった。また、従来は電話等で呼び出していたため、空港外にいる管理者は被害状況等の必要な情報を口頭でしか受けることができず、空港内にいるスタッフに対処すべき指示を伝えることが困難という問題があった。

【０００５】

また、これらの情報は迅速に提供する必要があるが、機密情報も含まれる可能性が高いため無条件に情報を提供すると情報がリークするという問題が発生する。機密性の高い情報、例えばハイジャックがあった場合の乗客の名簿、誘拐事件があった場合の情報等は、特定の人物にだけ通知すれば良く、第３者にはこれらの情報を提供する必要はない。かかる機密情報は、提供する人を確実に認証し、提供しても良い情報であるか否かの判断をした上で提供する必要があった。

【０００６】

また、これらの情報は事態の重要性に鑑み効率的に提供する必要がある。たとえば、事故が発生した場合は、まず全体の状況を提供し、そして死傷者の有無、警察等への手配の有無等、順序よく提供するのが望ましい。また、かかる事象は唐突に訪れるのが常であり、運航管理者または国家関係者等が睡眠中、運転中または外出中という場合もあるが、このような場合でも確実に情報を提供しなければならないという問題がある。さらに、睡眠中であれば、自動的にコンピュータを起動又はアラームを鳴らして注意を喚起する必要もある。また自宅にいれば、自宅に設置されているコンピュータへ情報を提供すれば事足りるが、外出中であれば携帯電話へ、運転中であれば車載コンピュータ等へ、というように異なるハードウェアへ情報を送信する必要があり、これらのハードウェアに適した情報を提供する必要がある。例えば、携帯電話であれば通信速度も遅く、また表示画面も小さいので、動画等のデータはフレーム数を大幅に減少して提供する必要がある。

【０００７】

本発明は係る事情に鑑みてなされたものであり、その目的とするところは、事象が発生した場合に、効率よく外部の管理者へ情報を送信でき、また情報の提供を受ける管理者の認証を確実に行い、さらに管理者の資格またはレベルに応じて提供すべき情報を制限することのできる機密性の高い危機管理システム及びコンピュータを提供することにある。

【０００８】

また、本発明の他の目的は、外部スタッフへ情報を提供する場合は、事象の種類の応じて、最適な順序で効率よく情報を提供可能な危機管理システム及びコンピュータを提供することにある。

【０００９】

また、本発明の他の目的は、外部の通信端末を自動的に起動すると共に、外部に設置されている通信端末の種類に応じて提供すべき情報を編集し、外部管理者の所在位置を問わず確実に情報の提供が可能な危機管理システム及びコンピュータを提供することにある。

【００１０】

【課題を解決するための手段】

第１発明にかかる危機管理システムは、通信網を介して接続されるサーバコンピュータと端末装置との間で実行され、所定の事象の発生により所要の情報を送受信する危機管理システムにおいて、前記サーバコンピュータは、事象に関する情報を受け付ける情報受付手段と、事象の種類と該事象毎の特性情報を登録した特性登録ファイルと、事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録した対処情報ファイルと、前記情報受付手段により受け付けた情報と前記特性登録ファイルとを比較して、事象を特定する特定手段と、該特定手段により特定した事象についての、前記対処情報ファイルに登録した提供情報項目に係る提供情報を収集する情報収集手段とを備え、前記端末装置は、管理者に付与される固有の識別子を受け付ける識別子受付手段と、管理者の人体特徴情報を受け付ける人体特徴情報受付手段と、前記識別子受付手段で受け付けた識別子及び前記人体特徴情報受付手段により受け付けた人体特徴情報を前記サーバコンピュータへ送信する識別情報送信手段とを備え、前記サーバコンピュータは、更に、管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録してある認証データファイルと、前記識別情報送信手段により送信された管理者の識別子及び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行う認証手段と、前記特定手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証手段により認証した管理者のアクセス許可レベルに基づいて提供情報に対するアクセスを許可するか否かを判断する判断手段と、該判断手段によりアクセスを許可すると判断した場合は、前記情報収集手段で収集した前記提供情報項目に係る提供情報を前記端末装置へ送信する提供情報送信手段とを備えることを特徴とする。

【００１１】

第２発明にかかる危機管理システムは、前記対処情報は前記複数の提供情報項目を提供すべき順序情報を更に含み、前記提供情報送信手段は、前記順序情報に従って前記提供情報を送信するよう構成してあることを特徴とする。

【００１２】

第３発明にかかる危機管理システムは、前記識別情報送信手段は、更に、前記端末装置のハードウェア情報を送信するよう構成してあり、前記提供情報送信手段は、前記判断手段によりアクセスを許可すると判断した場合は、前記提供情報送信手段により送信されたハードウェア情報に基づいて前記情報収集手段により収集した前記提供情報を編集した後に、前記端末装置へ前記編集後の提供情報を送信するよう構成してあることを特徴とする。

【００１３】

第４発明にかかるコンピュータは、他のコンピュータとの間で所定の事象の発生により所要の情報を送受信するコンピュータにおいて、事象に関する情報を受け付ける情報受付手段と、事象の種類と該事象毎の特性情報を登録した特性登録ファイルと、事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録した対処情報ファイルと、前記情報受付手段により受け付けた情報と前記特性登録ファイルとを比較して、事象を特定する特定手段と、該特定手段により特定した事象についての、前記対処情報ファイルに登録した提供情報項目に係る提供情報を収集する情報収集手段と管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録してある認証データファイルと、前記他のコンピュータから送信された管理者の識別子及び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行う認証手段と、前記特定手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証手段により認証した管理者のアクセス許可レベルに基づいて提供情報に対するアクセスを許可するか否かを判断する判断手段と、該判断手段によりアクセスを許可すると判断した場合は、前記情報収集手段で収集した前記提供情報項目に係る提供情報を前記他のコンピュータへ送信する提供情報送信手段とを備えることを特徴とする。

【００１４】

第５発明にかかるコンピュータは、他のコンピュータとの間で、事象の発生により必要な情報を送受信するコンピュータにおいて、管理者に付与される固有の識別子を受け付ける識別子受付手段と、管理者の人体特徴情報を受け付ける人体

特徴情報受付手段と、前記識別子受付手段で受け付けた識別子、前記人体特徴情報受付手段により受け付けた人体特徴情報及びハードウェア情報を送信する識別情報送信手段とを備えることを特徴とする。

【００１５】

第１発明、及び第４発明にあっては、まずサーバコンピュータは事象が発生した場合は、事象の種類、死傷者の有無等オペレータが入力した事象の情報を受け付ける。サーバコンピュータの特性登録ファイルには、予め過去の事例等に基づいて、事象毎（ハイジャック、離着陸事故、暴風雨などの緊急事態）の特性（例えば、ハイジャック犯の凶器の種類、死傷者の数、火災の有無、パイロットの状況、降水量、最大瞬間風速等）がテンプレートとして登録してあり、入力された事象の情報と特性情報ファイルとをパターンマッチング等の手法により比較して、現在発生している事象の種類を特定する。また、サーバコンピュータの対処情報ファイルには、事象の種類毎に、提供すべき情報の項目、及びその項目のアクセスレベル（機密性のレベル）が登録してある。そして、これを参照して特定した事象に関する提供情報を、収集する。収集する情報としては、空港事故（着陸失敗事故など）であれば、現場中継の画像情報、乗客名簿の情報、死傷者の情報及び代替便の情報などを収集する。そして、かかる情報を通信端末へ送信するようにしたので、空港外にいる運航管理者等の管理者は事象を迅速且つ容易に把握することが可能となる。また、これらの提供項目に係る情報は上述のように、アクセスレベルが登録されており、例えば提供を受ける者が運航管理者（アクセス許可レベル最高）であれば全ての情報の提供を受けることができ、提供を受ける者が単に旅行代理店の代理人（アクセス許可レベル中）であれば、アクセスレベルの高い情報（例えば、現場中継の情報または機密情報など）にはアクセスできず、アクセスレベルの低い情報（例えば乗客名簿の情報または代替便の情報など）の提供しか受けることができない。このように提供を受ける者のアクセス許可レベルによって、提供情報の閲覧を制限することとしたので機密性を保持することが可能となる。また、通信端末には、固有のＩＤ及び指紋または音声等の受付手段を設けて、これらの情報をサーバコンピュータへ送信して、情報を受けようとする者の正当性を認証すると共にアクセス許可レベルをもチェックする。この

ように、本システムでは、情報の提供を受ける者の正当性及びアクセス許可レベルをバイオメトリック認証により認証することとしたので、極めてセキュリティの高い情報提供システムを提供することが可能となる。

【００１６】

第２発明にあっては、サーバコンピュータから通信端末へ送信する提供情報を、予め登録してある提供順序に従って送信する。例えば、飛行機事故であれば、提供情報「現場状況の画像情報」を順序情報「１」、提供情報「事故の経緯情報」を順序情報「２」、提供情報「死傷者の有無情報」を「３」…という如く重要性に応じて予め順序情報が登録してあり、この順序に従い逐次情報を送信するのである。このように、提供情報を重要度に応じて送信するようにしたので、外部にいる管理者は情報を効率よく把握することが可能となる。また、例えば、買い物等で管理者が外出しており、順序「１」および「２」までは携帯電話（通信端末）で情報を受信し、急いで自宅に帰って自宅の通信端末を起動した場合は、順序に従った情報「３」、「４」…が続いて表示されるので、迅速また効率的に情報を入手することが可能となる。

【００１７】

第３発明及び第５発明にあっては、認証の情報を通信端末からサーバコンピュータへ送信する際に、通信端末のハードウェア情報を送信する。たとえば、通信端末が携帯電話である場合は、その携帯電話の機種コード等の情報を送信する。そして、その情報を受け取ったサーバコンピュータは、送信先のハードウェアのスペックに応じて提供情報を編集する。例えば、送信先の通信端末が携帯電話である場合は、通信速度は遅く、またメモリも少ないので、動画像はフレーム数を大幅に減少して送信し、またテキストデータは何度かに分けて送信する。このように、送信先のハードウェアの種類に応じて送信内容を編集するようにしたので、外部にいる管理者は、情報を受信するハードウェアの種類を問わず受信することが可能となり、自宅外においても確実に情報を受信することが可能となる。

【００１８】

【発明の実施の形態】

以下本発明をその実施の形態を示す図面に基づいて詳述する。

【００１９】

実施の形態１

図１は本発明に係る危機管理システムを示す模式図である。図において１は危機管理情報を集中的に管理するサーバコンピュータである。サーバコンピュータは例えば図のように飛行場等に設置されており、テレビカメラ等から出力される画像データの記録、乗客名簿の記憶等情報の収集及び、通信端末２ａ、２ａ…、通信端末２ｂ、２ｂ…または通信端末２ｃ、２ｃ…、又は図示しない警察等の機関への情報の送信を行う。サーバコンピュータ１は通信網Ｗを介して、例えば空港外の管理者（運航管理者、旅行代理店の代理人、パイロット、警察官、消防士、官僚等）の住居等に設置される通信端末２ａ、２ａ…、携帯電話等の通信端末２ｂ、２ｂ…及び車載用の通信端末２ｃ、２ｃ…（以下、通信端末２という）接続されている。

【００２０】

図２はサーバコンピュータ１のハードウェア構成を示すブロック図である。図において１２は通信網Ｗを介して通信端末２、２…と情報を送受信する通信部である。サーバコンピュータ１にはキーボード等の入力部１４が設けられ、空港内にいるオペレータは事象が発生した場合は被害状況を表示部１７を見ながら入力する（図３参照）。ＭＰＵ１１は入力された事象に関する情報をＲＡＭ１３に格納する。また、ハードディスク等の記憶部１５には各種ファイルが記憶されている。なお、これらファイルの詳細は後述する。また、現場で発生している事故等を撮影する場合、ＭＰＵ１１はビデオカメラ等の撮像部１６を制御し、画像データを記憶部１５の画像データファイル１５ｃに記憶する。

【００２１】

図３は事象の情報を入力部１４から入力する際の表示部１７の表示画面を示す説明図である。事象が発生した場合は、空港内にいるオペレータは図３に示すブラウザに現在の状況をそれぞれ入力部１４より入力する。まず、事象が何であるかを特定するために、列挙されているタブ（ハイジャック、空港事故、天災など）から１のタブ選択する。なお、図３ではハイジャックタブを選択した場合について表示してある。入力項目としては死傷者数、乗客数、犯人が所有する武器の

種類等を入力する。また、ボックスにはない入力事項については不足データテキストボックスに直接文字を入力する。例えば、ハイジャックによりフランス人が負傷した場合は、フランス語の理解できる医師を準備する必要があるのでその旨を記載する。その他、代替便が必要な場合は便番号等を入力するようにしても良い。

【００２２】

図４は事例データファイル１５ｈのデータベース構造を示す説明図である。事例データファイル１５ｈには世界各国で発生した事象についての被害状況、及びどのようにしてトラブルを解決したか等の情報が蓄積されている。これらの情報はオペレータが入力部１４より逐次入力し蓄積する。例えば図４のように、事象を空港事故、ハイジャック又は天災等に分類し、続いて日時、被害状況、死傷者数等を入力する。又、その事象の際にとった解決手段を登録する。例えば、対応手順、解決のポイント及び警察又は病院等の関連機関との対応を登録する。

【００２３】

図５は特性登録ファイル１５ａのデータベース構造を示す説明図である。特性登録ファイル１５ａは、オペレータが事例データファイル１５ｈを参照して各事象の特性、つまり事象のモデルをテンプレートとして登録したものである。図５に示すとおりハイジャックには様々なケースが想定されるため、いくつかのテンプレートを登録している。ＭＰＵ１１は図３において入力しＲＡＭ１３に格納した諸データと、登録しているテンプレートとをパターンマッチング等の手法により比較し、一致又は近似するテンプレートを特定する。これにより、事象の種類（例えばハイジャック政治犯ＴＹＰＥ・Ｂ等）が特定される。

【００２４】

記憶部１５の一部領域には事象の種類に応じて設けられる、提供情報項目及びそのアクセスレベルが登録された対処情報ファイル１５ｂが設けられている。図６は対処情報ファイル１５ｂのデータベース構造を示す説明図である。対処情報ファイル１５ｂには事象の種類（ハイジャック政治犯ＴＹＰＥ・Ｂ，…天災台風ＴＹＰＥ・Ａなど）に応じて予め複数の提供情報項目が登録されている。例えば、事象の種類をハイジャック政治犯ＴＹＰＥ・Ｂと特定した場合、撮像部１６で

撮像した現場の中継画像（現場中継）、便の出発時刻・到達時刻・便の番号・貨物船であるか・乗客数等の便詳細情報、及び死傷者・火災の有無等の被害状況などを、項目として登録しておく。

【００２５】

これらの提供情報項目にはそれぞれ情報を公開するに当たってのしきい値、つまりアクセスレベルが設けられている。外部にいる運航管理者のように、空港内の全ての情報を把握する必要がある者に対しては最高のアクセス許可レベル（例えば３）が付与されている。一方、単なる旅行代理店の代理人等には機密情報を提供する必要はないので低いアクセス許可レベル（例えば１）が付与される。一方、提供情報項目にもそれぞれアクセスレベルが登録してあり、例えば現場中継又は被害状況等の機密性を保持する必要がある項目はアクセスレベル３と登録されている。逆に、乗客名簿等は旅行代理店の代理人に開示しても良いのでアクセスレベル１と登録されている。旅行代理店の代理人等はアクセス許可レベルが１であるのでアクセスレベルが１以下の情報しか提供されない（アクセスレベル２，３の情報は提供されない）。一方、運航管理者等のアクセス許可レベルが３の者はアクセスレベルが３以下の情報、つまり全ての情報の提供を受けることが可能となる（アクセスレベル１から３全て提供可能）。これにより、機密情報が確実に保護されることとなる。

【００２６】

さらに、対処情報ファイル１５ｂには情報を提供すべき順序が予め登録されている。図６に示すとおり、まず初めに、ＳＴＥＰ１の情報「現場中継」、ついでＳＴＥＰ２の情報「便詳細」というように通信端末２へ情報を送信する際の順序情報も予め登録されている。そして、事象の種類が特定された場合は、提供すべき情報を収集する。収集する提供情報項目は対処情報ファイル１５ｂを参酌して行う。たとえば、事象の種類が「ハイジャック政治犯ＴＹＰＥ・Ｂ」であると「現場中継」及び「便詳細」等の情報を収集する。「現場中継」情報の収集は撮像部１６より撮像したハイジャック現場の画像を記憶部１５の画像データファイル１５ｃに記録する。「便詳細」情報については航空便の詳細が登録された航空便情報ファイル１５ｄを参酌して収集する。また、対処情報ファイル１５ｂの提供

情報項目にない不足している情報を収集する。不足情報は図３におけるテキストボックスに入力された内容に基づいて情報を収集する。そしてこれらの収集した情報を収集情報ファイル１５ｇに登録するのである。

【００２７】

また、仮に事象の種類が「天災台風ＴＹＰＥ・Ａ」であれば、現場中継情報の他に、図示しない気象予報データベース等から気象状況を収集する。そしてＭＰＵ１１は、これらの収集した情報を収集情報ファイル１５ｇに記憶し、この記憶した内容を予め定められたアクセスレベル及び順序に従って逐次通信端末２へ送信するのである。なお、ＲＡＭ１３は、情報が逐次送信される度に、順序情報を更新する。例えば、ＳＴＥＰ１の「現場中継」情報がまず送信された場合は「１」と記憶し、ＳＴＥＰ２の「便詳細」情報が送信された場合はインクリメントして「２」と記憶する。このように構成することで何らかの原因により、情報の送信が中断しても次の情報（ＳＴＥＰ３の「被害状況」情報）を時系列的に送信することが可能となる。なお、不足情報については、そのアクセスレベル及び順序情報についてはオペレータが入力して適当な値を付与するようにすればよい。

【００２８】

図７はハードウェア情報登録部１５ｆのデータベース構造を示す説明図である。ハードウェア情報登録部１５ｆには、情報提供先の通信端末２，２…の画面サイズ、色数、内部メモリ等のスペックが登録されている。つまり、情報提供先の通信端末２が十分なＣＰＵとメモリを備えるコンピュータ等の通信端末２ａであれば何ら支障はないが、携帯電話等の通信端末２ｂへ情報を送信する際は、その性能に応じてデータ量を編集する必要があるのである。通信端末２が情報の提供を求めてサーバコンピュータ１へ、受信要求パケットを送信する場合は、このパケットにはハードウェア情報（例えば機種コード）も含まれており、ＭＰＵ１１はこの送信されたハードウェア情報及びハードウェア情報登録部１５ｆに基づいて、収集情報ファイル１５ｇに記憶した各提供情報を編集する。例えば、通信端末２ｂ（携帯電話）から受信要求があった場合、現場中継に係る動画データであれば、１秒間に送信するフレーム数を５フレーム程度に減少させる。また、乗客名簿等も１度にデータを送信するのではなく、複数回に分割して送信するように

する。

【００２９】

図８は認証データファイル１５ｅのデータベース構造を示す説明図である。認証データファイル１５ｅには、情報の提供を受ける管理者（運航管理者、旅行代理店の代理人、パイロット、警察官、消防士、官僚等）の固有の識別子（ＩＤ）、役職、氏名、パスワード等が登録されている。また、第３者のなりすましを防止するために、予め人体特徴情報、例えば、本人の指紋、音声、網膜のパターン等を登録しておく。つまり、通常の識別子及びパスワード認証に加えてバイオメトリック認証を行うことによって機密情報の漏洩防止を強化したものである。さらに、アクセス許可レベルが予め登録されてあり、この登録されているアクセス許可レベルに基づいて、空港外部にいる管理者は必要な情報を享受することができる。

【００３０】

図９は通信端末２のハードウェア構成を示すブロック図である。図において２２はサーバコンピュータ１との間で情報を送受信する通信部である。事象が発生しサーバコンピュータ１のＭＰＵ１１から、事象発生信号が送信されてきた場合は、スイッチ回路等の電力給断装置２５はスイッチをオンにして通信端末２へ電力を供給し、通信端末２を起動する。起動後ＭＰＵ２１は、スタッフに注意を喚起すべく、図示しない警報部のアラームをならすと共に、事象の発生を示す情報を表示部２４に表示する。このように、電力給断装置２５を設け、異常が発生した場合は、通信端末２を起動し、事象の発生を強制的に通知するようにしたので、情報が確実に伝達することができると共に省エネルギ化を図ることが可能となる。

【００３１】

つづいて、ＭＰＵ２１は、表示部２４に「識別子（ＩＤ）、パスワード及び指紋を入力して下さい」と表示する。キーボード、タッチパネル、指紋読み取り機等の入力部２３に必要な情報が入力された場合、ＭＰＵ２１はこれらの情報を受け付けてサーバコンピュータ１へ送信する。なお、認証方法については後述する。認証を終え、サーバコンピュータ１からアクセスレベルを満たす提供情報が逐

次送信されてきた場合、ＭＰＵ２１はその内容を記憶部２６に記憶すると共に表示部２４に表示する。これらの情報は、入力部２３の操作によりいつでも呼び出すことが可能である。さらに、図示しないＧＰＳ等の位置計測部を設けて、空港外にいる管理者の所在地を計測し、その計測情報をサーバコンピュータ１で管理するようにしてもよい。

【００３２】

図１０は空港外にいる管理者の認証処理の手順を示すフローチャートである。まず、入力部２３から入力された識別子及びパスワードを受け付ける（ステップＳ１０１）。ついで、入力された指紋等の人体特徴情報を受け付ける（ステップＳ１０２）。そして、識別子、パスワード及び人体特徴情報をサーバコンピュータ１へ送信する（ステップＳ１０３）。もちろん、識別子、パスワード及び人体特徴情報は別々に送信するようにしても良い。これらの情報を受信したサーバコンピュータ１のＭＰＵ１１は、認証データファイル１５ｅを参照して識別子及びパスワードが正当であるか否かを判断する（ステップＳ１０４）。判断した結果、一致しないと判断した場合は（ステップＳ１０４でＮＯ）、不正アクセスであるとして、アクセスを拒否又は再度入力を求める（ステップＳ１０５）。

【００３３】

一方、判断した結果、一致すると判断した場合は（ステップＳ１０４でＹＥＳ）、認証データファイル１５ｅに登録されている指紋と、送信されてきた指紋とを比較して正当であるか否かを判断する（ステップＳ１０６）。一致しないと判断した場合は（ステップＳ１０６でＮＯ）、第３者によるなりすましである可能性が高いので、不正アクセスであるとして、アクセスを拒否又は再度の入力を求める（ステップＳ１０７）。判断した結果、一致すると判断した場合は（ステップＳ１０６でＹＥＳ）、正当なユーザであるとして提供すべき情報を通信端末２へ送信する（ステップＳ１０８）。なお、本実施の形態では識別子の認証をまず初めに行い、続いて指紋等の人体特徴情報を認証することとしたが、これに限らず、まず、人体特徴情報を認証し、その後識別子（パスワードも含む）の認証を行うようにしても良い。又、認証をすべてサーバ側で行うのではなく、例えば指紋等の人体特徴情報による認証は専用のＩＣカードシステム等を利用して通信端

末２側で行うようにしても良い。

【００３４】

図１１はサーバコンピュータ１における事象の特定及び情報収集の処理手順を示すフローチャートである。まず、事象が発生した場合は、オペレータが入力した事象に関する情報（図３参照）を受け付ける（ステップＳ１１１）。そしてこの受け付けた情報と特性登録ファイル１５ａに登録してある特性情報とをパターンマッチング等の手法により比較し（ステップＳ１１２）、最も近似する事象の種類を特定する（ステップＳ１１３）。事象が決まった後は、対処情報ファイル１５ｂを参酌して、現在発生中の事象に係る提供情報項目を抽出する（ステップＳ１１４）。たとえば、現在発生中の事象がハイジャック政治犯ＴＹＰＥ・Ｂである場合、提供情報項目「現場中継」、「便詳細」、被害状況」等を抽出する。そして、ＭＰＵ１１は抽出した提供すべき情報を収集し（ステップＳ１１５）、その収集した情報を収集情報ファイル１５ｇに逐次記憶する。例えば、情報の収集が「現場中継」であれば、画像データファイル１５ｃに記憶している画像データのうち、事故発生の瞬間から現在までの記憶データを収集情報ファイル１５ｇに記憶する（ステップＳ１１７）。また「便情報」の収集は航空便情報ファイル１５ｄを参照して、顧客名簿等を収集し収集情報ファイル１５ｇにその内容を記憶する（ステップＳ１１７）。また、提供情報項目にない提供情報（不足情報）が存在する場合は、オペレータが入力追加して（ステップＳ１１６）、その内容を同様に収集情報ファイル１５ｇに記憶する。不足情報としては、例えばフランス語に対応できる医師が必要である旨の情報、代替便の情報等である。なお、これらの不足情報の入力に際しては、オペレータはそのアクセスレベル及び順序情報を同時に入力する。このようにテンプレートとして登録されていない情報もフレキシブルに追加して提供するようにしたので、十分な情報を管理者へ提供することが可能となる。

【００３５】

図１２及び図１３は本発明に係る危機管理システムの処理手順を示すフローチャートである。まず事象が発生した場合、サーバコンピュータ１は通信端末２ａ…、２ｂ…及び２ｃ…へ事象の発生信号を同報で送信する（ステップＳ１２１）

。発生信号を受信した電力給断装置２５は、発生信号をトリガーとしてスイッチをオンにし、通信端末２へ電力を供給する（ステップＳ１２２）。これにより通信端末２は強制的に起動される（ステップＳ１２２）。または、発信音（アラーム）を強制的に発して、事象の発生を通知する（ステップＳ１２２）。事象を認識した空港外にいる管理者は、通信端末２から認証情報を送信する（ステップＳ１２３）。認証情報送信パケットは、識別子、パスワード、人体特徴情報、のほか通信端末２のハードウェア情報が送信される（ステップＳ１２３）。具体的には、機種名等のコード番号が送信される。

【００３６】

このようにして送信された認証情報は、ステップＳ１０１からステップＳ１０８で説明した手順で認証を行う（ステップＳ１２４）。サーバコンピュータ１はこの認証の後又は認証と並行して事象の特定、提供情報の収集等ステップＳ１１１からステップＳ１１７で説明した処理を行う（ステップＳ１２５）。そして次のステップへ移行する（Ａ）。

【００３７】

続いて、図６に示す提供情報項目に係る提供情報を、アクセスレベル制限を加えながら、通信端末２へ送信する。まず、ＲＡＭ１３に「ＳＴＥＰ・ｉ」＝１と記憶する（ステップＳ１３１）。そして、ＳＴＥＰ・１の（図６の例では現場中継）アクセスレベルと送信されてきた管理者のアクセス許可レベルとを比較し、管理者のアクセス許可レベルが項目ｉ（１）のアクセスレベル以上であるか否かを判断する（ステップＳ１３２）。管理者のアクセス許可レベルが項目ｉのアクセスレベル以上である場合は（ステップＳ１３２でＹＥＳ）、ハードウェア情報登録部１５ｆを参照して通信端末２のハードウェア情報を認識する（ステップＳ１３３）。そして、提供情報（現場中継情報）を編集し、編集後の提供情報を通信端末２へ送信する（ステップＳ１３４）。例えば、管理者が買い物に出かけており、携帯電話（通信端末２ｂ）で情報の受信を要求した場合は、ハードウェア情報は携帯電話であり、ＭＰＵ１１はハードウェア情報登録部１５ｆを参照して、画像データのフレーム数調整、圧縮等の編集を行った後、その編集後の内容を送信するのである。

【００３８】

一方、管理者のアクセス許可レベルが項目ｉのアクセスレベル以上でない場合は（ステップＳ１３２でＮＯ）、その情報を秘密にする必要があるので情報を送信しない。そして、次のＳＴＥＰ・ｉ＋１の情報を提供するために、ＲＡＭ１３に格納している「ＳＴＥＰ・ｉ」をインクリメントする（ステップＳ１３８）。そして、インクリメント後の「ＳＴＥＰ・ｉ」が情報提供最大数Ｎに達したかどうかを判断する（ステップＳ１３９）。即ち、図６における提供情報項目の全てを提供し終えた（ＳＴＥＰ・Ｎ）のか否かを判断するのである。ここで、まだ提供すべき情報が存在する場合、つまり「ＳＴＥＰ・ｉ」がＮでない場合は（ステップＳ１３９でＮＯ）、ステップＳ１３２へ移行し処理を繰り返す。一方、「ＳＴＥＰ・ｉ」がＮに達した場合（ステップＳ１３９でＹＥＳ）、全ての情報を送信し終えたので、全ての処理を終了する。

【００３９】

上述の説明では通信端末２が、情報の送受信の途中で機種が変更（例えば携帯電話から自宅のコンピュータへ変更）することはなかったが、機種変更される場合もあるので、以下に、機種変更された際の処理を説明する。例えば、買い物中に通信端末２ｂ（携帯電話）で、事象の発生を知りＳＴＥＰ・ｉまで情報を受信し、そして、自宅に戻り自宅の通信端末２ａにハードウェアが切り替わったとする。ステップＳ１３４により提供情報が送信されたのち、ハードウェアが変更された場合（ステップＳ１３５）、再度管理者が認証を行うために、認証情報をサーバコンピュータ１へ送信する（ステップＳ１３６）。認証を行った後（ステップＳ１３７）、ＳＴＥＰ・ｉをインクリメントする（ステップＳ１３８）。

【００４０】

そして、ステップＳ１３２に移行しアクセスレベル以上であると判断した場合（ステップＳ１３２でＹＥＳ）、ステップＳ１３６で送信されたハードウェア情報とハードウェア情報登録部１５ｆとに基づいてハードウェア情報を認識する（ステップＳ１３３）。そしてハードウェア変更後の情報に基づいて提供情報を編集し、ＳＴＥＰ・ｉ＋１の情報を変更後の通信端末２へ送信する（ステップＳ１３４）。以上のように構成することで、ハードウェアが変更された後でも、変更

後のハードウェアに応じた情報提供が可能となると共に、既に受信を受けた情報ＳＴＥＰ・１からＳＴＥＰ・ｉについては、再び受信する必要がなくなるので、スピーディに情報を得ることが可能となる。なお、本実施の形態では既に取得した情報を入手しないこととしているが、もちろん他のハードウェアで受信した提供情報を受信するようにしても良い。また、通信端末２にＧＰＳ等の図示しない位置計測部を設け、通信端末２ｂ（携帯電話）が自宅付近に近づいたと判断した場合は、その情報をサーバコンピュータ１へ送信し、サーバコンピュータ１は管理者が自宅に到着する前に情報を先に送信しておくようにしても良い。さらに、本実施の形態では危機管理を空港に関するものとして説明したが、これに限らず、国家レベルでの緊急情報管理、地震発生時の危機管理、警察管又は消防士に対する危機管理であっても良いことはもちろんである。

【００４１】

実施の形態２

図１４は実施の形態２に係る危機管理システムの構成を示す模式図である。サーバコンピュータ１には、図１４に示す、入力される情報を受け付けさせ、特性を登録させ、対処情報を登録させ、事象の種類を特定させ、提供すべき情報を収集させ、認証データを登録させ、その認証データに基づいて認証を行わせ、アクセスレベル以下であるか否かを判断させ、さらに提供情報を送信させるプログラムが記憶された記録媒体１ａ（ＣＤ－ＲＯＭ、ＭＯ又はＤＶＤ－ＲＯＭ等）がサーバコンピュータ１のハードディスク等の記憶部１５にインストールされている。かかるプログラムはサーバコンピュータ１のＲＡＭ１３にロードして実行される。これにより、上述のような本発明のサーバコンピュータ１として機能する。

【００４２】

本実施の形態２は以上の如き構成としてあり、その他の構成及び作用は実施の形態１と同様であるので、対応する部分には同一の参照番号を付してその詳細な説明を省略する。

【００４３】

（付記１）　通信網を介して接続されるサーバコンピュータと端末装置との間で実行され、所定の事象の発生により所要の情報を送受信する危機管理システムに

おいて、

前記サーバコンピュータは、

事象に関する情報を受け付ける情報受付手段と、

事象の種類と該事象毎の特性情報を登録した特性登録ファイルと、

事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録した対処情報ファイルと、

前記情報受付手段により受け付けた情報と前記特性登録ファイルとを比較して、事象を特定する特定手段と、

該特定手段により特定した事象についての、前記対処情報ファイルに登録した提供情報項目に係る提供情報を収集する情報収集手段と

を備え、

前記端末装置は、

管理者に付与される固有の識別子を受け付ける識別子受付手段と、

管理者の人体特徴情報を受け付ける人体特徴情報受付手段と、

前記識別子受付手段で受け付けた識別子及び前記人体特徴情報受付手段により受け付けた人体特徴情報を前記サーバコンピュータへ送信する識別情報送信手段と

を備え、

前記サーバコンピュータは、更に、

管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録してある認証データファイルと、

前記識別情報送信手段により送信された管理者の識別子及び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行う認証手段と、

前記特定手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証手段により認証した管理者のアクセス許可レベルに基づいて提供情報に対するアクセスを許可するか否かを判断する判断手段と、

該判断手段によりアクセスを許可すると判断した場合は、前記情報収集手段で収集した前記提供情報項目に係る提供情報を前記端末装置へ送信する提供情報送

信手段と

を備えることを特徴とする危機管理システム。（請求項１）

【００４４】

（付記２）　前記対処情報は前記複数の提供情報項目を提供すべき順序情報を更に含み、

前記提供情報送信手段は、

前記順序情報に従って前記提供情報を送信するよう構成してある

ことを特徴とする付記１に記載の危機管理システム。（請求項２）

（付記３）　前記識別情報送信手段は、

更に、前記端末装置のハードウェア情報を送信するよう構成してあり、

前記提供情報送信手段は、

前記判断手段によりアクセスを許可すると判断した場合は、前記提供情報送信手段により送信されたハードウェア情報に基づいて前記情報収集手段により収集した前記提供情報を編集した後に、前記端末装置へ前記編集後の提供情報を送信するよう構成してある

ことを特徴とする付記１または２に記載の危機管理システム。（請求項３）

【００４５】

（付記４）　前記端末装置へ供給する電力を給断する電力給断装置

を更に備え、

前記サーバコンピュータは、

事象の発生信号を前記電力給断装置へ送信する発生信号送信手段

を更に備え、

前記電力給断装置は、

前記発生信号送信手段により送信された発生信号に基づいて前記端末装置へ電力を供給する供給手段

を備えることを特徴とする付記１乃至３に記載の危機管理システム。

（付記５）　他のコンピュータとの間で所定の事象の発生により所要の情報を送受信するコンピュータにおいて、

事象に関する情報を受け付ける情報受付手段と、

事象の種類と該事象毎の特性情報を登録した特性登録ファイルと、

事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録した対処情報ファイルと、

前記情報受付手段により受け付けた情報と前記特性登録ファイルとを比較して、事象を特定する特定手段と、

該特定手段により特定した事象についての、前記対処情報ファイルに登録した提供情報項目に係る提供情報を収集する情報収集手段と、

管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録してある認証データファイルと、

前記他のコンピュータから送信された管理者の識別子及び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行う認証手段と、

前記特定手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証手段により認証した管理者のアクセス許可レベルに基づいて提供情報に対するアクセスを許可するか否かを判断する判断手段と、

該判断手段によりアクセスを許可すると判断した場合は、前記情報収集手段で収集した前記提供情報項目に係る提供情報を前記他のコンピュータへ送信する提供情報送信手段と

を備えることを特徴とするコンピュータ。（請求項４）

【００４６】

（付記６）　前記対処情報は前記複数の提供情報項目を提供すべき順序情報を更に含み、

前記提供情報送信手段は、

前記順序情報に従って前記提供情報を送信するよう構成してある

ことを特徴とする付記５に記載のコンピュータ。

（付記７）　前記提供情報送信手段は、

前記判断手段によりアクセスを許可すると判断した場合は、前記他のコンピュータから送信された該他のコンピュータのハードウェア情報に基づいて前記情報収集手段により収集した前記提供情報を編集した後に、前記他のコンピュータへ

前記編集後の提供情報を送信するよう構成してある

ことを特徴とする付記５または６に記載のコンピュータ。

（付記８）　他のコンピュータとの間で、事象の発生により必要な情報を送受信するコンピュータにおいて、

管理者に付与される固有の識別子を受け付ける識別子受付手段と、

管理者の人体特徴情報を受け付ける人体特徴情報受付手段と、

前記識別子受付手段で受け付けた識別子、前記人体特徴情報受付手段により受け付けた人体特徴情報及びハードウェア情報を送信する識別情報送信手段と

を備えることを特徴とするコンピュータ。（請求項５）

【００４７】

（付記９）　他のコンピュータとの間で所定の事象の発生により所要の情報を送受信させるコンピュータプログラムが記録されており、コンピュータでの読み取りが可能な記録媒体において、

前記コンピュータに、事象に関する情報を受け付けさせる情報受付プログラムコード手段と、

前記コンピュータに、事象の種類と該事象毎の特性情報を登録させる特性登録プログラムコード手段と、

前記コンピュータに、事象の種類に応じた、複数の提供情報項目及び該提供情報項目毎に定めたアクセスレベルを含む対処情報を登録させる対処情報プログラムコード手段と、

前記コンピュータに、前記情報受付プログラムコード手段により受け付けた情報と前記特性登録プログラムコードにより受け付けた情報とを比較し、事象を特定させる特定プログラムコード手段と、

前記コンピュータに、前記特定プログラムコード手段により特定させた事象についての、前記対処情報プログラムコード手段により登録した提供情報項目に係る提供情報を収集させる情報収集プログラムコード手段と、

前記コンピュータに、管理者毎に予め識別子、人体特徴情報及びアクセス許可レベルを含む認証データを登録させる認証登録プログラムコード手段と、

前記コンピュータに、前記他のコンピュータから送信された管理者の識別子及

び人体特徴情報、並びに前記認証データファイルに登録してある識別子及び人体特徴情報に基づいて管理者の認証を行わせる認証プログラムコード手段と、

前記コンピュータに、前記特定プログラムコード手段により特定した事象に係る提供情報項目のアクセスレベル及び前記認証プログラムコード手段により認証した管理者のアクセス許可レベルに基づいて、提供情報に対するアクセスを許可するか否かを判断させる判断手段と、

前記コンピュータに、該判断プログラムコード手段によりアクセスを許可すると判断した場合は、前記情報収集プログラムコード手段で収集した前記提供情報項目に係る提供情報を前記他のコンピュータへ送信させる提供情報送信プログラムコード手段と

を含むコンピュータプログラムが記録されていることを特徴とするコンピュータでの読み取り可能な記録媒体。

【００４８】

【発明の効果】

以上の詳述した如く、第１発明、及び第４発明にあっては、まずサーバコンピュータは事象が発生した場合は、事象の種類、死傷者の有無等オペレータが入力した事象の情報を受け付ける。サーバコンピュータの特性登録ファイルには、予め過去の事例等に基づいて、事象毎（ハイジャック、離陸事故、暴風雨などの緊急事態）の特性（例えば、ハイジャック犯の凶器の種類、死傷者の数、火災の有無、パイロットの状況、降水量、最大瞬間風速等）がテンプレートとして登録してあり、入力された事象の情報と特性情報ファイルとをパターンマッチング等の手法により比較して、現在発生している事象の種類を特定する。また、サーバコンピュータの対処情報ファイルには、事象の種類毎に、提供すべき情報の項目、及びその項目のアクセスレベル（機密性のレベル）が登録してある。そして、これを参照して特定した事象に関する提供情報を、収集する。収集する情報としては、空港事故（着陸失敗事故など）であれば、現場中継の画像情報、乗客名簿の情報、死傷者の情報及び代替便の情報などを収集する。そして、かかる情報を通信端末へ送信するようにしたので、空港外にいる運航管理者等の管理者は事象を迅速且つ容易に把握することが可能となる。また、これらの提供項目に係る情報

は上述のように、アクセスレベルが登録されており、例えば提供を受ける者が最高管理者（アクセス許可レベル最高）であれば全ての情報の提供を受けることができ、提供を受ける者が単に旅行代理店の代理人（アクセス許可レベル中）であれば、アクセスレベルの高い情報（例えば、現場中継の情報または機密情報など）にはアクセスできず、アクセスレベルの低い情報（例えば乗客名簿の情報または代替便の情報など）の提供しか受けることができない。このように提供を受ける者のアクセス許可レベルによって、提供情報の閲覧を制限することとしたので機密性を保持することが可能となる。また、通信端末には、固有のＩＤ及び指紋または音声等の受付手段を設けて、これらの情報をサーバコンピュータへ送信して、情報を受けようとする者の正当性を認証すると共にアクセス許可レベルをもチェックする。このように、本システムでは、情報の提供を受ける者の正当性及びアクセス許可レベルをバイオメトリック認証により認証することとしたので、極めてセキュリティの高い情報提供システムを提供することが可能となる。

【００４９】

第２発明にあっては、サーバコンピュータから通信端末へ送信する提供情報を、予め登録してある提供順序に従って送信する。例えば、飛行機事故であれば、提供情報「現場状況の画像情報」を順序情報「１」、提供情報「事故の経緯情報」を順序情報「２」、提供情報「死傷者の有無情報」を「３」…という如く重要性に応じて予め順序情報が登録してあり、この順序に従い逐次情報を送信するのである。このように、提供情報を重要度に応じて送信するようにしたので、外部にいる管理者は情報を効率よく把握することが可能となる。また、例えば、買い物等で管理者が外出しており、順序「１」および「２」までは携帯電話（通信端末）で情報を受信し、急いで自宅に帰って自宅の通信端末を起動した場合は、順序に従った情報「３」、「４」…が続いて表示されるので、迅速また効率的に情報を入手することが可能となる。

【００５０】

第３発明及び第５発明にあっては、認証の情報を通信端末からサーバコンピュータへ送信する際に、通信端末のハードウェア情報を送信する。たとえば、通信端末が携帯電話である場合は、その携帯電話の機種コード等の情報を送信する。

そして、その情報を受け取ったサーバコンピュータは、送信先のハードウェアのスペックに応じて提供情報を編集する。例えば、送信先の通信端末が携帯電話である場合は、通信速度は遅く、またメモリも少ないので、動画像はフレーム数を大幅に減少して送信し、またテキストデータは何度かに分けて送信する。このように、送信先のハードウェアの種類に応じて送信内容を編集するようにしたので、外部にいる管理者は、情報を受信するハードウェアの種類を問わず受信することが可能となり、自宅外においても確実に情報を受信することが可能となる等、本発明は優れた効果を奏し得る。

【図面の簡単な説明】

【図１】

本発明に係る危機管理システムを示す模式図である。

【図２】

サーバコンピュータのハードウェア構成を示すブロック図である。

【図３】

事象の情報を入力部から入力する際の表示部の表示画面を示す説明図である。

【図４】

事例データファイルのデータベース構造を示す説明図である。

【図５】

特性登録ファイルのデータベース構造を示す説明図である。

【図６】

対処情報ファイルのデータベース構造を示す説明図である。

【図７】

ハードウェア情報登録部のデータベース構造を示す説明図である。

【図８】

認証データファイルのデータベース構造を示す説明図である。

【図９】

通信端末のハードウェア構成を示すブロック図である。

【図１０】

空港外にいる管理者の認証処理の手順を示すフローチャートである。

【図１１】

サーバコンピュータにおける事象の特定及び情報収集の処理手順を示すフローチャートである。

【図１２】

本発明に係る危機管理システムの処理手順を示すフローチャートである。

【図１３】

本発明に係る危機管理システムの処理手順を示すフローチャートである。

【図１４】

実施の形態２に係る危機管理システムの構成を示す模式図である。

【符号の説明】

１　　サーバコンピュータ

１５ａ　特性登録ファイル

１５ｂ　対処情報ファイル

１５ｅ　認証データファイル

１５ｆ　ハードウェア情報登録部

１５ｇ　収集情報ファイル

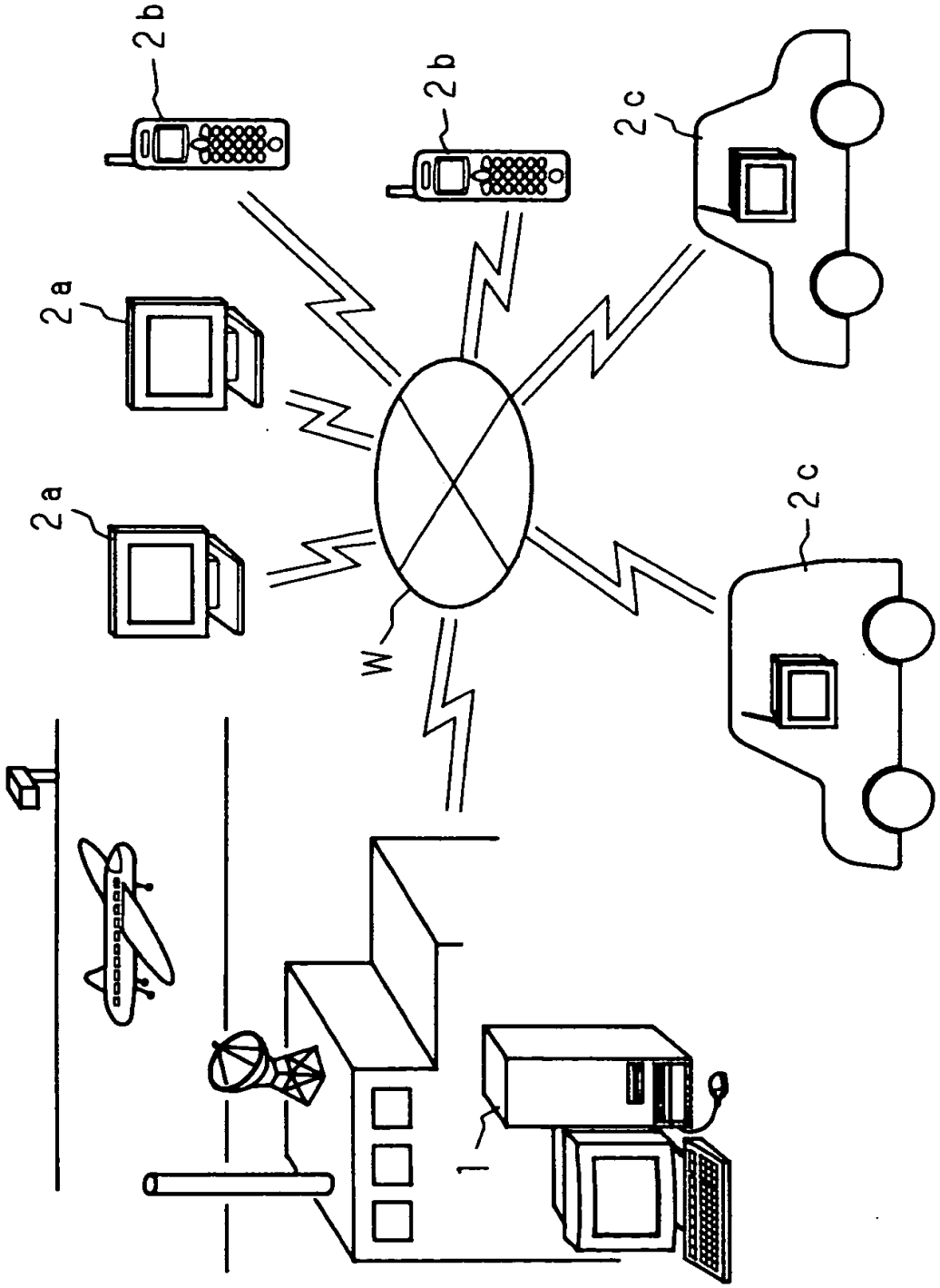
２ａ、２ｂ、２ｃ　通信端末

Ｗ　　通信網

【書類名】　　図面

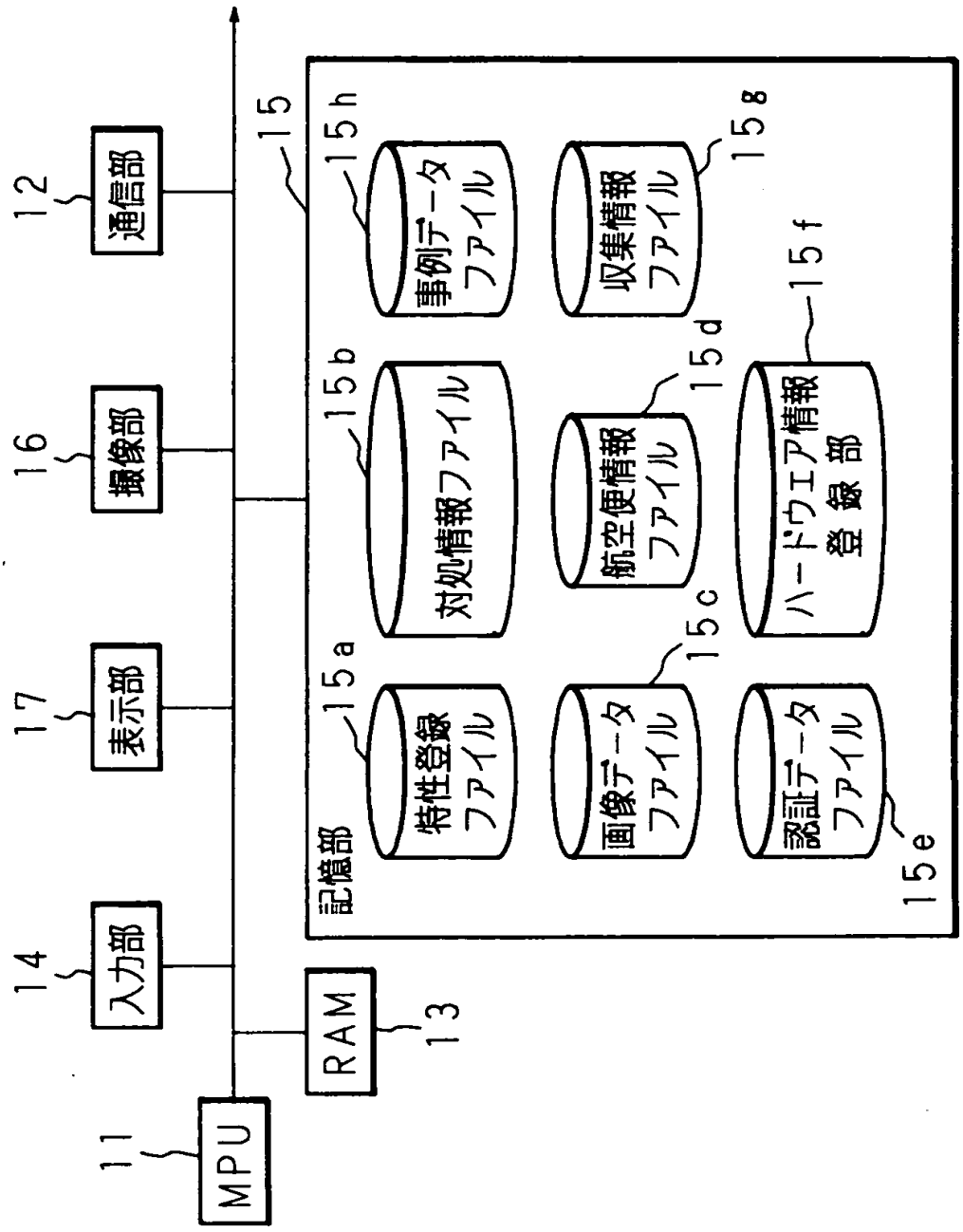
【図１】

本発明に係る危機管理システムを示す模式図



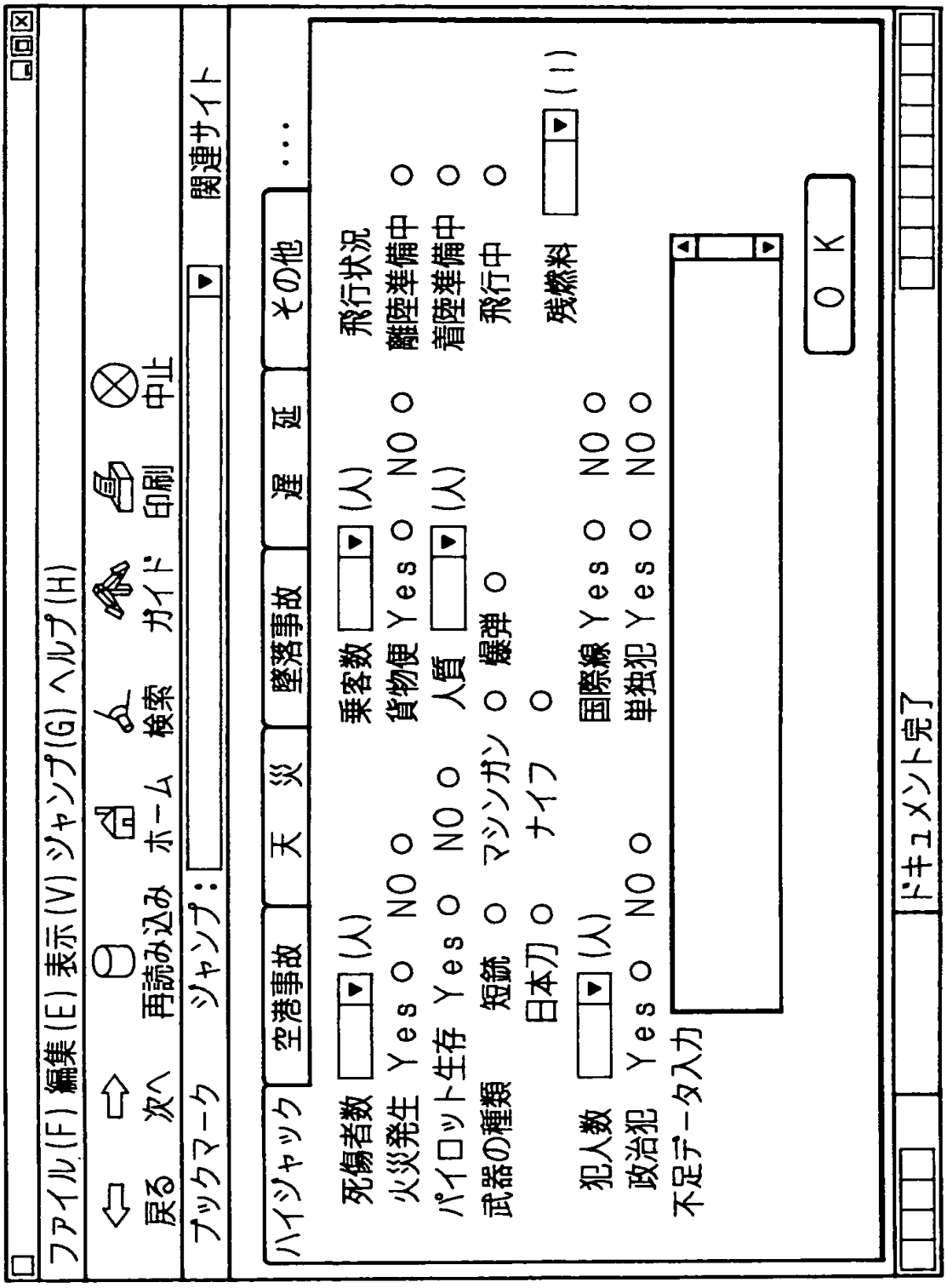
【図２】

サーバコンピュータのハードウェア構成を示すブロック図



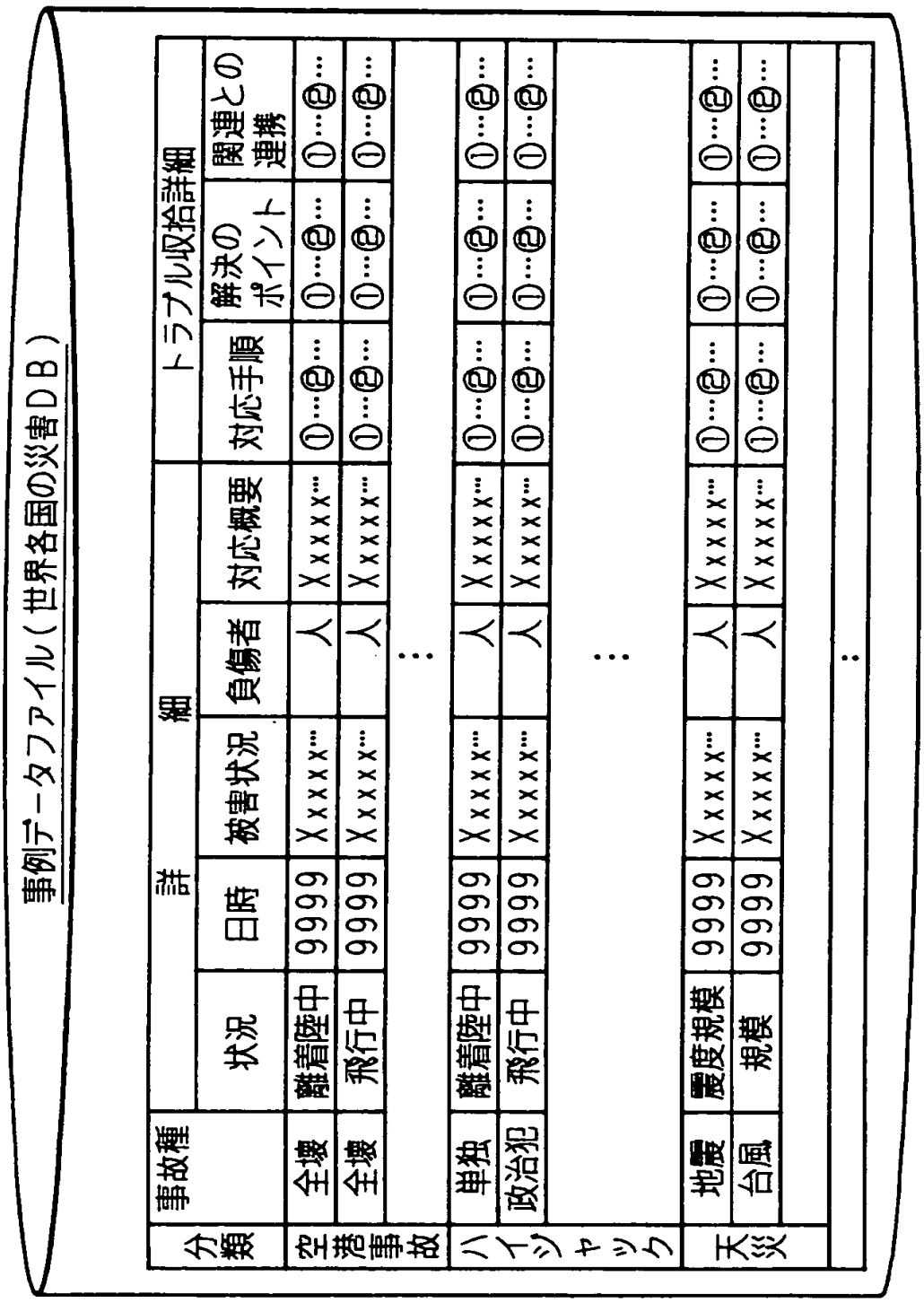
【図３】

事象の情報を入力部から入力する際の表示部の表示画面を示す説明図



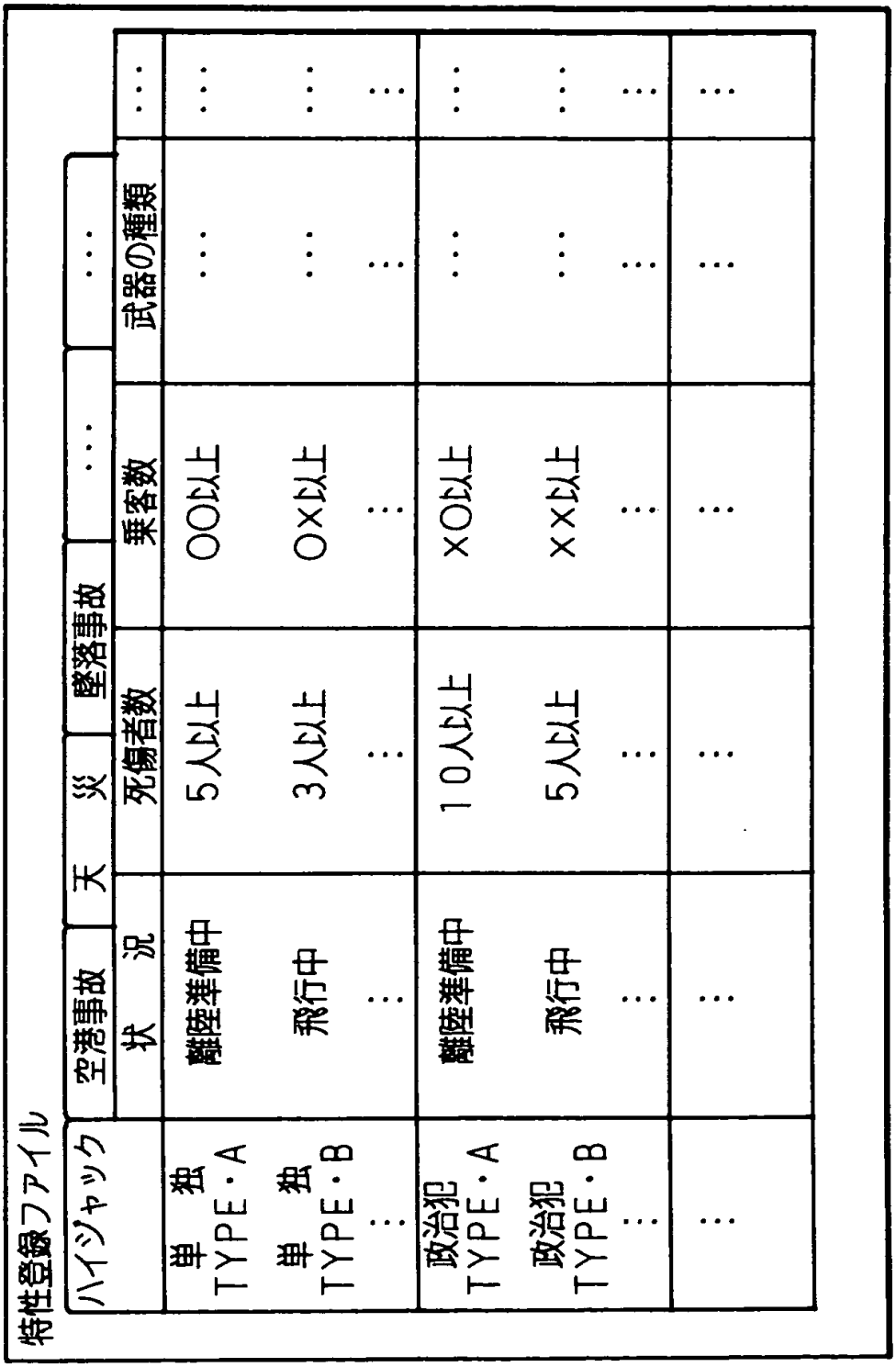
【図４】

事例データファイルのデータベース構造を示す説明図



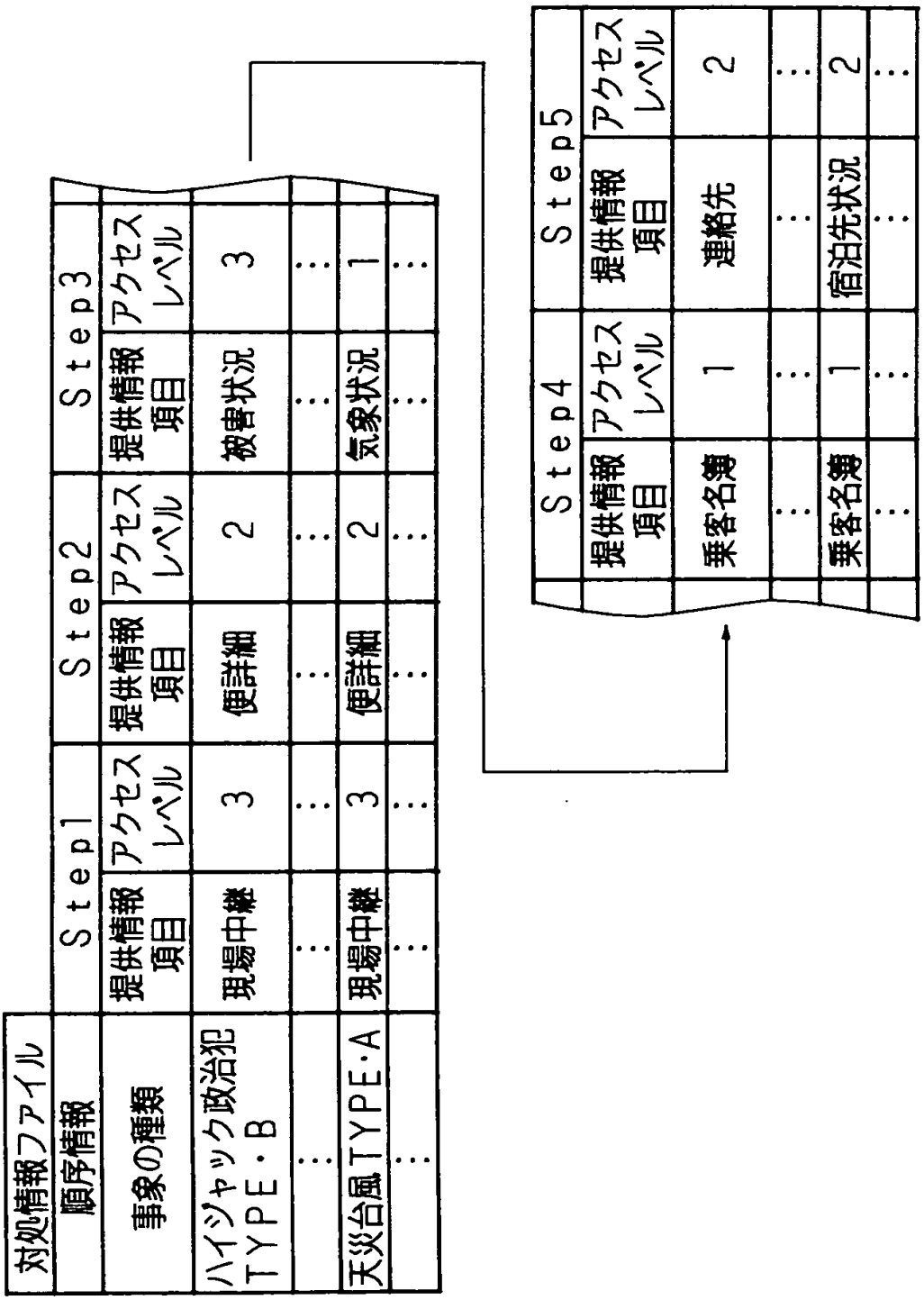
【図５】

特性登録ファイルのデータベース構造を示す説明図



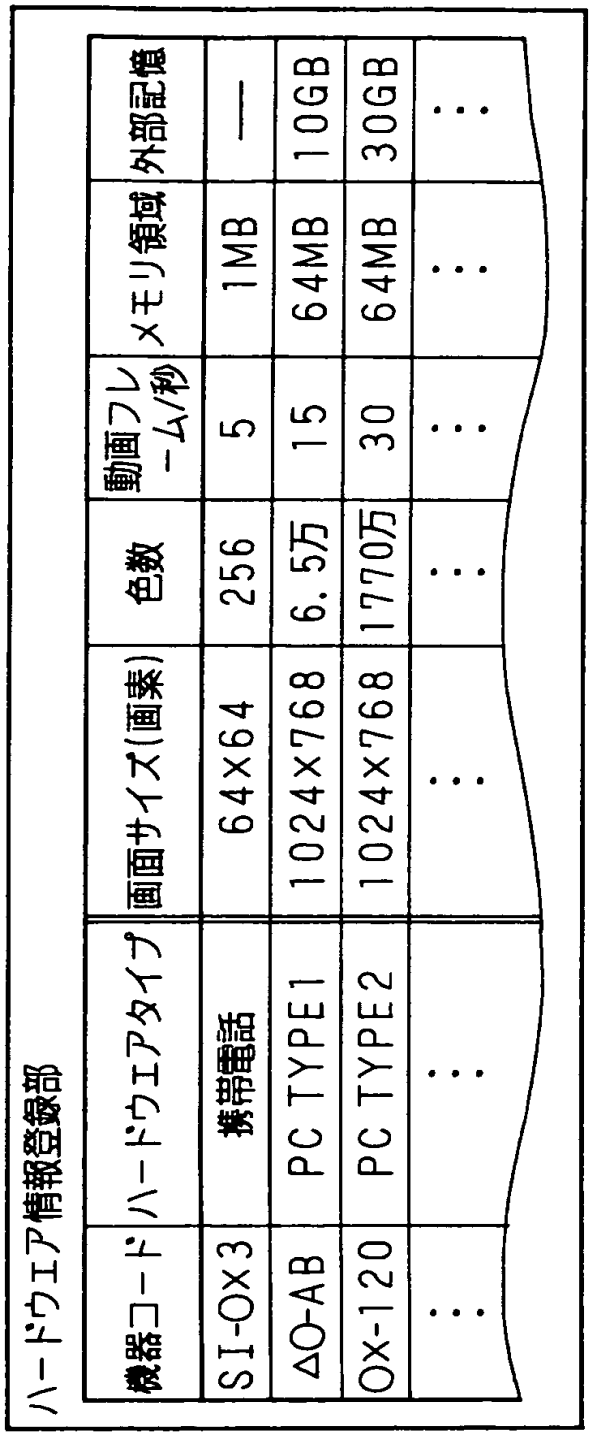
【図６】

対処情報ファイルのデータベース構造を示す説明図



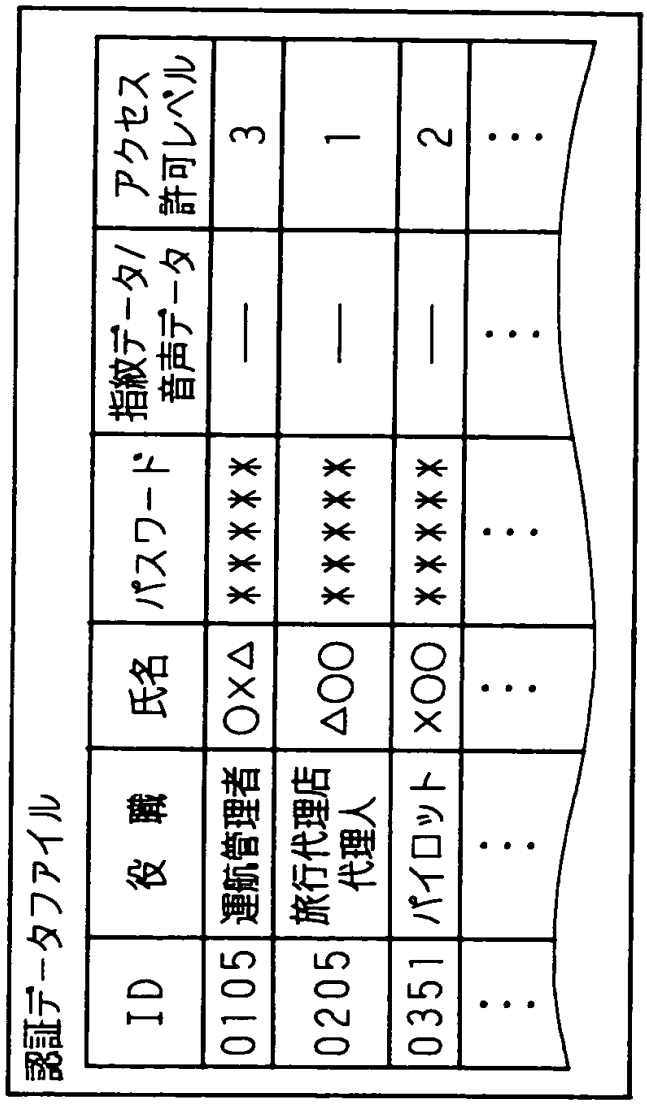
【図７】

ハードウエア情報登録部のデータベース構造を示す説明図



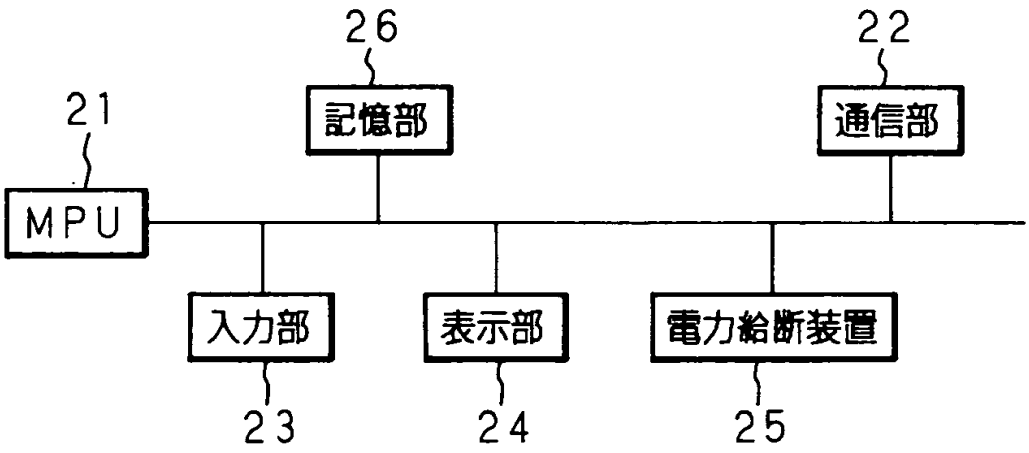
【図８】

認証データファイルのデータベース構造を示す説明図



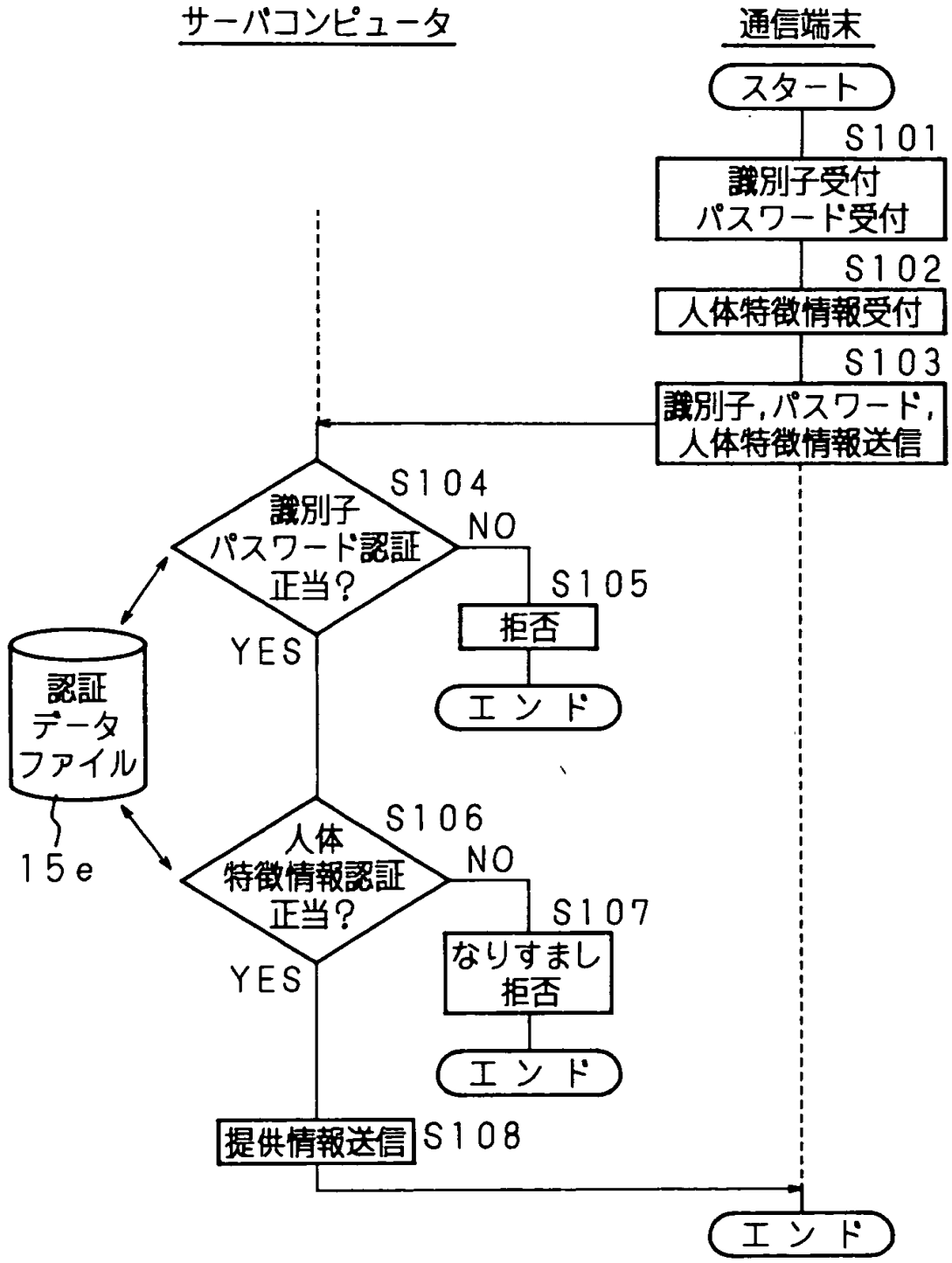
【図９】

通信端末のハードウエア構成を示すブロック図



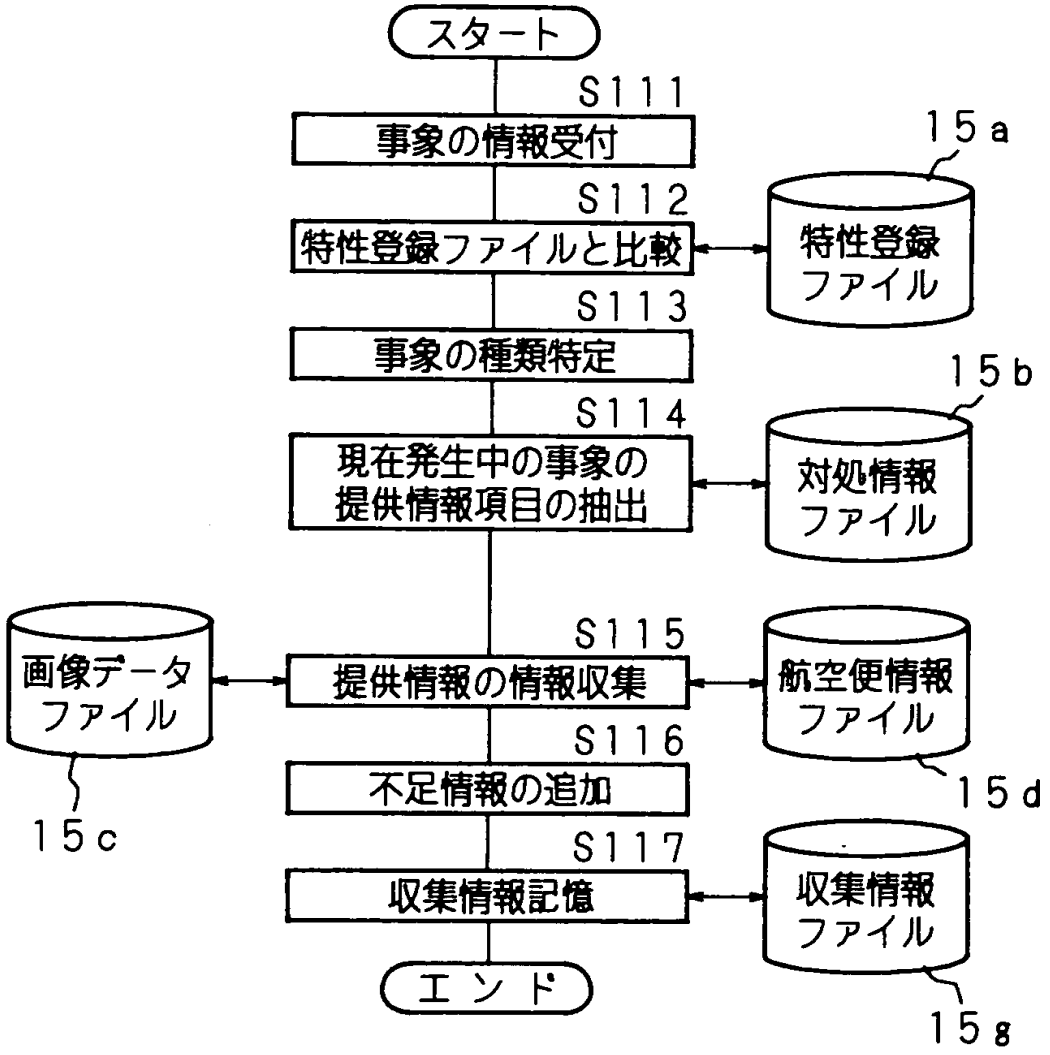
【図１０】

空港外にいる管理者の認証処理の手順を示すフローチャート



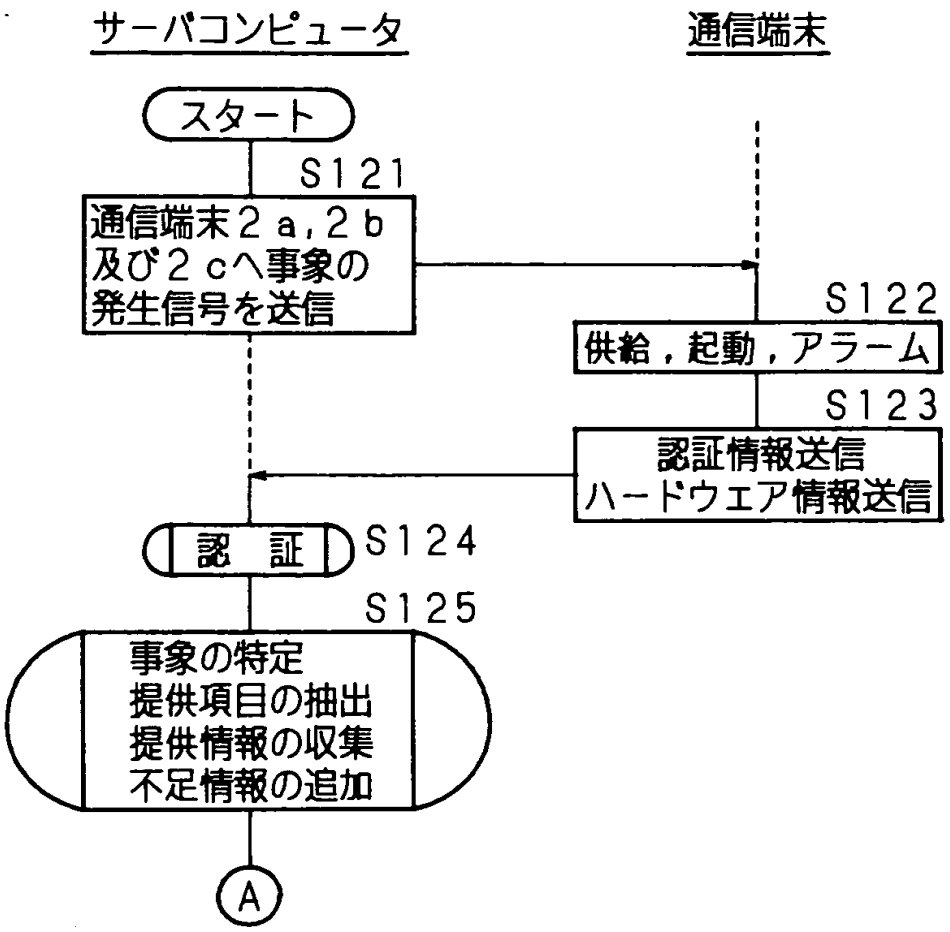
【図１１】

サーバコンピュータにおける事象の特定及び情報収集の処理手順を示すフローチャート



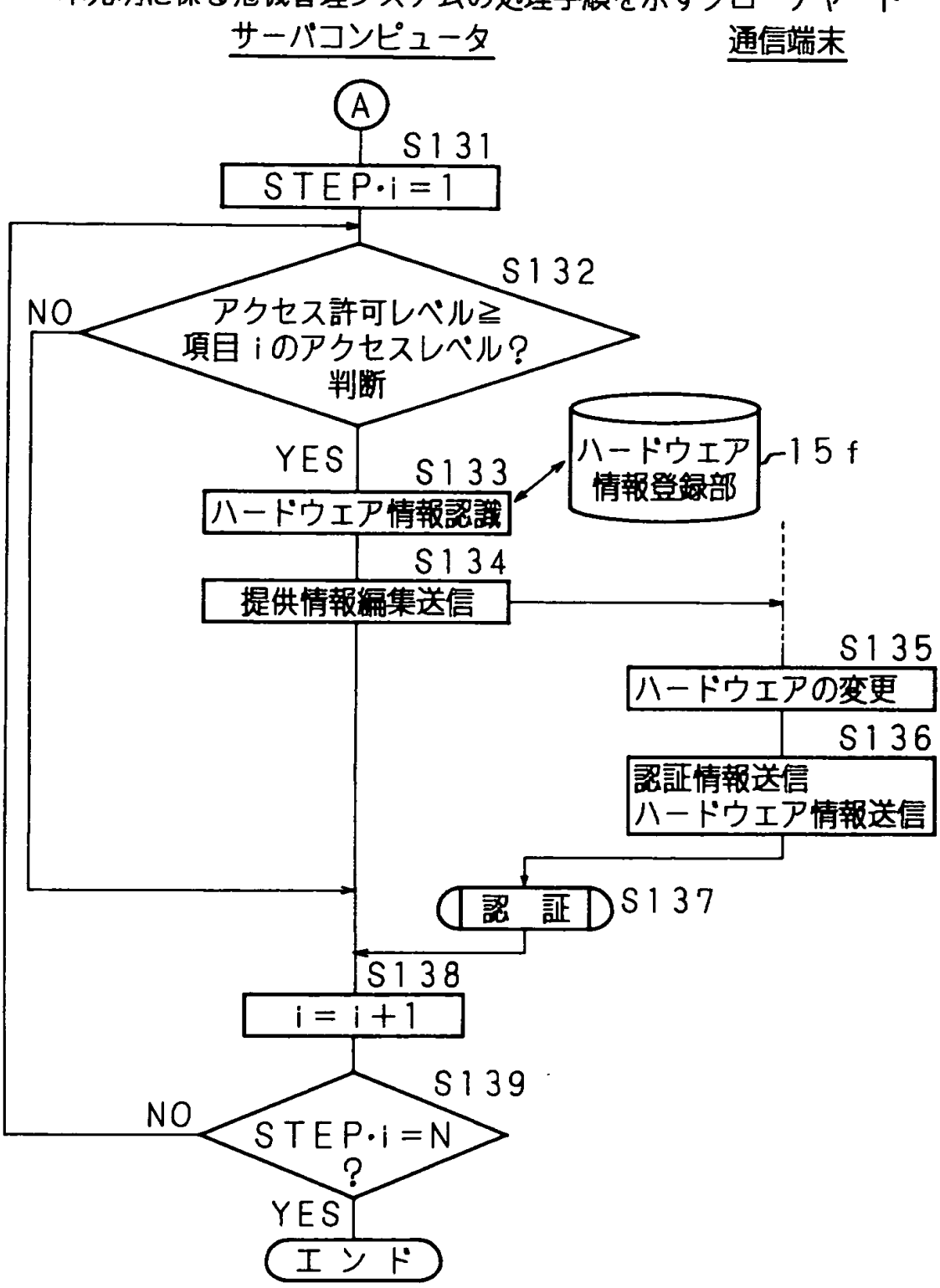
【図１２】

本発明に係る危機管理システムの処理手順を示すフローチャート



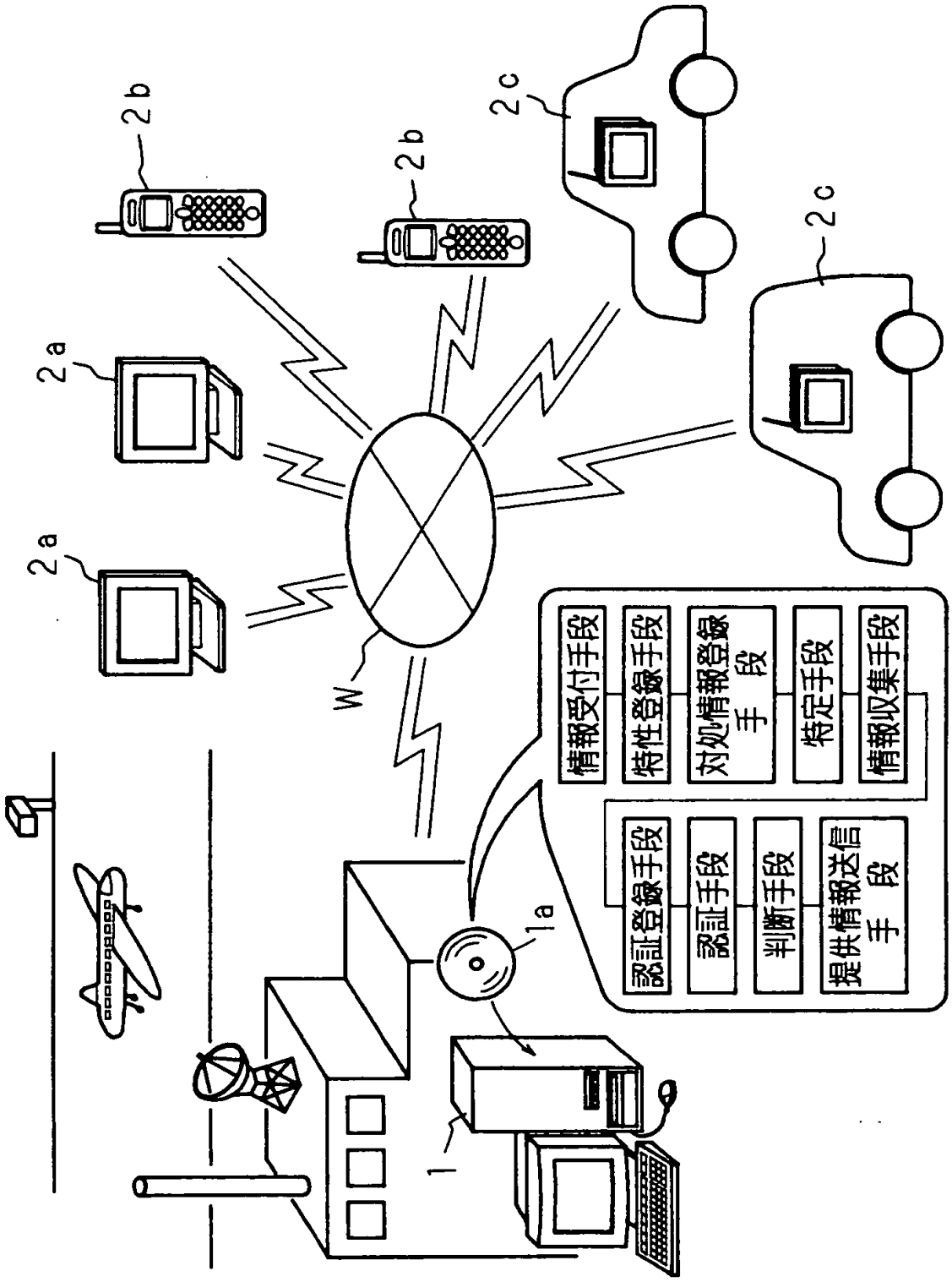
【図１３】

本発明に係る危機管理システムの処理手順を示すフローチャート



【図１４】

実施の形態２に係る危機管理システムの構成を示す模式図



【書類名】　　要約書

【要約】

【課題】　緊急事態が発生した場合、情報は効率よく、また迅速に提供する必要があるが、機密情報も含まれるため無条件に情報を提供すると情報がリークするという問題があった。

【解決手段】　サーバコンピュータ１は事象をシミュレートし、通信端末２ａ、２ｂ、２ｃへ提供すべき情報を的確に抽出し、情報を収集する。そして、人体特徴情報及びアクセス許可レベルに基づいて認証を行うことによってセキュリティを強化する。また、情報の提供は順序情報に基づいて効率的に行うと共に、送信先のハードウェア情報を収集することにより編集してから実行する。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　〔０００００５２２３〕

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社